Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A validation protocol for determining whether an untrusted authentication chip is valid, or not, including the steps of:

generating an original random number; ~~and~~

applying, in the trusted authentication chip, ~~encrypting it with~~ an asymmetric encryption encrypted random number;

passing the encrypted random number to an untrusted authentication chip;

decrypting, in the untrusted authentication chip, the encrypted random number with an asymmetric decryption function using a second secret key from the untrusted authentication chip to produce a decrypted random number; ~~in the untrusted authentication chip~~;

comparing the decrypted random number with the original random number, without knowledge of the second secret key, and in the event of a match considering the untrusted chip to be valid; and,

otherwise considering the untrusted chip to be invalid.

2. (Original) A validation protocol according to claim 1, where the random number is not secret, but where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed.

3. (Original) A validation protocol according to claim 1, where the first key is a public key.

4. (Original) A validation protocol according to claim 1, where the encryption is implemented in software.

5. (Original) A validation protocol according to claim 1, where the encryption is implemented in a second authentication chip.

6. (Original) A validation protocol according to claim 1, where the keys used for encryption and decryption are 2048 bits or larger.

7. (Currently amended) A validation system for determining whether an untrusted authentication chip is valid, or not, where the system comprises:

a random number generator to generate an original random number;

an asymmetric encryptor to encrypt ~~generated~~ the original random numbers using a first key in a trusted authentication chip~~and a first key for the encryptor~~;

an untrusted authentication chip ~~which~~ to receives the encrypted random number, the untrusted chip including an asymmetric decryption function to decrypt the encrypted random numbers ~~and~~ using a second secret key for the decryption function to produce a decrypted random number; and

comparison means to compare the decrypted random number with the original random number, without knowledge of the second secret key;

whereby, in the event of a match between the decrypted random number and the original random number, the untrusted chip is considered to be valid; otherwise the untrusted chip is considered to be invalid.

8. (Original) A validation system according to claim 7, where the random number generator, encryptor and comparison means are in an external system.

9. (Currently amended) A validation system according to claim 8, where the external system is in a device in which ~~are~~ it is mounted, and the untrusted chip is in ~~the~~ a consumable product.

10. (Original) A validation system according to claim 7, where the random number generator and encryptor are in a second authentication chip, and the comparison means are in an external system which receives the random number and the encrypted version before passing only the encrypted version to the untrusted chip; the system also receives back the decrypted version from the untrusted chip and performs the comparison.

11. (Original) A validation system according to claim 10, where the system is in a device in which consumables are mounted, and the untrusted chip is in the consumable.

12. (Original) A validation system according to claim 7, where the random number is not secret, but the random number generator includes a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed.

13. (Original) A validation system according to claim 7, where the first key is a public key.

14. (Original) A validation system according to claim 7, where the encryption is implemented in software.

15. (Original) A validation system according to claim 7, where the encryption is implemented in a second authentication chip.

16. (Original) A validation system according to claim 7, where the keys used for encryption and decryption are 2048 bits or larger.